Bogotá, D.C.

Ministerio de las Tecnologías de la Información y las Comunicaciones
Sylvia Constaín
Ministra

REF: Comentarios al borrador de CONPES de seguridad digital

La Fundación Karisma, la Fundación para la Libertad de Prensa y el Centro de Estudios Internet y Sociedad de la Universidad del Rosario (ISUR) presentamos comentarios conjuntos al borrador de la *Política Nacional de Confianza y Seguridad Digital*, con el animo de aportar y mejor el documento.

El borrador de esta polítca publicada para comentarios tiene por objetivo "mejorar las capacidades actuales del país en seguridad digital para generar confianza y adaptación para el futuro digital" a través de un plan de acción en cinco puntos: (1) adecuación del marco de gobernanza de seguridad digital y (2) del marco institucional de seguridad digital para mejorar la participación; (3) la adaptación del marco legal y regulatorio, (4) el fortalecimiento de las capacidades en seguridad digital de las organizaciones y (5) de la ciudadanía.

Este borrador muestra un desarrollo positivo en términos de incluir, por primera vez, el reconocimiento de la falta de datos sobre el estado de la situación de seguridad digital del sector social y de grupos vulnerables. Además, se admiten las brechas de capacidades y conocimiento al no haberse incorporado enfoques diferencial y de género en las estrategias gubernamentales que buscan "elevar la participación de las mujeres, líderes sociales, comunidades étnicas, en el ámbito de la seguridad digital".

También apreciamos que se hayan observado las barreras existentes en el país frente a la divulgación coordinada de vulnerabilidades, que impiden a la ciudadanía en general apoyar los esfuerzos nacionales a favor de un ecosistema digital confiable y seguro.

A pesar de los esfuerzos evidentes del documento por hacer un diagnóstico y proponer unas acciones adecuada a la situación institucional de la seguridad digital en el país, es necesario apuntar algunos elementos que representan oportunidades de mejora para que esta política incluya visiones más garantistas de los derechos humanos.

Diagnóstico y definiciones

RECOMENDACIONES

1. Revisar la definición de seguridad digital para que que enfatice la relación entre derechos humanos y la orientación de la política en esta materia.
2. Incluir expresamente los principios del CONPES 3854 de 2016 en la nueva versión de la política.

El diagnóstico aún sigue teniendo un enfoque muy centrado en el impacto económico de un ciberespacio seguro, sin reconocer los impactos sociales y humanos. Esto, quizá, se deba a que aún no pone a la persona en el centro, lo que tiene implicaciones directas en cómo se desarrolla la política. Y este borrador, sigue mostrando un fuerte enfoque militar y reactivo. No hay nada más que ver el papel que se le asignó al Ministerio de Defensa, a la que se le han asignado actividades que, cuando menos, levanta sospechas y alarmas.

Si la política reconociera que "[l]a seguridad digital y los derechos humanos son complementarios, se refuerzan mutuamente y son interdependientes"[1], muy probablemente la política tendría su núcleo en la protección de las personas y, consecuentemente, de los derechos humanos. Evidentemente, este no es el caso cuando, además, la definición de seguridad, adoptada en el Conpes de 2016 y que se mantiene sin cambios en este borrador, se centra exclusivamente en proteger al Estado:

> ***Seguridad digital:*** *es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.*

Invitamos a revisar la definición para que refuerce relación entre seguridad digital y derechos humanos para promover un ciberespacio seguro y libre. En ese sentido, la definición propuesta por el Grupo de Trabajo 1 (WG1, por sus siglas en inglés) de la *Freedom Online Coalition* (FOC) presenta un buen balance al respecto y, tal vez, pueda servir de guía:

> *La ciberseguridad es la preservación, a través de políticas, tecnología y educación, de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente a fin de mejorar la seguridad de las personas tanto online como offline.*[2]

[1] FOC-WG1 (s.f.). *An Internet Free and Secure: A Human Rights Approach to Cybersecurity Policy-making*. Disponible en https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Narrative-Final-28-April-2016.pdf

[2] FOC-WG1. (2014). Recommendations for Human Rights Based Approaches to Cybersecurity. Disponible en https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf.

Aprovechamos también para cuestionar la inclusión de una segunda definición –en este caso, llamada ciberseguridad–, que se presenta desde una perspectiva de seguridad nacional:

> ***Ciberseguridad:*** *es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.*

Hay que destacar que esta definición es más cerca a la del FOC, aunque todavía presenta problemas al dirigirse a usuarios, una clasificación que deshumaniza y desconoce que la seguridad digital debe diseñarse para proteger a las personas, independientemente de quien sean. De otra parte, siendo este documento la política en la materia, todas las entidades gubernamentales deben operar bajo la misma definición. Se espera de esta política que ofrezca un mismo marco de operación.

Finalmente, nos parece importante que el documento incluya una recopilación de principios. Es cierto que en algún punto se infiere que los principios del anterior CONPES, cuya validez vence a final de este año, siguen vigentes para este e incluso se hace referencia a ellos en una de las actividades de la línea de acción 4 del Objetivo específico 4.3.2. Sin embargo, nos parece que una política, aun cuando sea solo una actualización, debería incluir una sección de principios.

Marco de gobernanza

RECOMENDACIONES

1. Reconocer la oportunidad que presenta esta nueva política de definir una estructura institucional y reducir la dispersión y ambigüedad en las competencias de las entidades involucradas hasta ahora.
2. Definir con mayor precisión el tipo de organización institucional que seguirá la política de seguridad digital. Específicamente, precisar el rol y las responsabilidades de entidades como el Ministerio de Defensa, de las TIC y del Coordinador Nacional y el Comité de Seguridad Digital.
3. Hacer una distinción clara entre los objetivos de la Agenda Nacional de Seguridad Digital y la política propuesta. No es claro cuál es la función y alcance de cada uno respecto a la definición de objetivos estratégicos y el marco institucional de la seguridad digital.
4. Crear una línea de acción dentro del objetivo de adecuación del marco institucional (4.3.1) para analizar la conveniencia de que el colCERT siga suscrito al Ministerio de Defensa y pueda pasar a ser una entidad independiente para tener un carácter civil e incrementar la confianza en la institucionalidad de la seguridad digital.

Esta nueva política tiene como objetivo general el mejoramiento de la confianza y adaptación para el futuro digital. Para ello, busca adecuar sus marcos de gobernanza, institucionales y legales/regulatorios, además de fortalecer capacidades. En otras palabras, uno de los propósitos principales es reordenar la casa.

El marco de gobernanza que se intenta adecuar, no obstante, aún queda bastante difuso y complejo. La Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) recomienda que cuando se trabaja en este aspecto se definan, entre otros:[3]

- Los roles, responsabilidades y mecanismo de rendición de cuenta de todos los actores relevantes.
- El marco para el diálogo y coordinación de las diversas actividades emprendidas en la estrategia nacional de seguridad digital.
- La entidad o grupo de trabajo interagencial o interministerial encargada.
- La estructura de esa entidad o grupo de trabajo, sus responsabilidades y su relación con otros actores.

Además, señala que hay diferentes estructura de gobernanza. Algunos enfoquen optan por depender de una autoridad central de seguridad digital con amplias responsabilidades y competencias; mientras, otros se caracterizan por un alto grado de cooperación entre entes públicos. Actualmente, el enfoque descentralizado es el que prevalece en el país. El diagnóstico que presenta el borrador parece privilegiar la estructura centralizada. No obstante, sabemos las dificultades técnicas, administrativas, humanas y financieras de crear una agencia o entidad especializada. Las líneas de acción 1 y 2 también dejan entrever que, de momento, lo mejor es fortalecer el mecanismo de coordinación nacional que existe con miras a instaurar un instancia central encargada de la materia.

Es necesario definir las entidades involucradas y sus responsabilidades de acuerdo a sus mandatos institucionales en la gobernanza de la política de seguridad digital. Tener roles y responsabilidades claras ayudaría a establecer una definición única de seguridad digital y aclararía especialmente los roles de los ministerios de Defensa y TIC. En ocasiones, no es claro si por definición estos ministerios se disputan con el Coordinador Nacional y con el Comité de Seguridad Digital. Lo anterior no tiene por qué competir con la actividad 1 de modificación de la conformación y funciones del Comité de Seguridad Digital, que hace parte de la Línea de Acción 2 del Objetivo específico 3.4.1. Muy al contrario, ayudaría a darle un mejor lineamiento a esa acción si se tiene definido el papel y las responsabilidades generales del Comité de Seguridad Digital.

Esto también ayudaría a aclarar a qué se refiere la actividad 4 de la Línea de Acción 2 del Objetivo específico 3.4.1 cuando menciona que el Coordinador Nacional creará una “Agenda Nacional de Seguridad Digital”. Hay poca distinción entre el objetivo de esta agenda y el propio

[3] ENISA. (2016). *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies*. Disponible en https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Conpes. Más allá de cómo se le llame a este documento, la importancia está en definir con mayor claridad que se está hablando de un plan de trabajo o plan maestro para el futuro cumplimiento de los objetivos y acciones que se trazan en la política. También ayudaría si simplificaran las actividades del Conpes para hacerlas más flexibles, de manera que sirvan de guía en búsqueda de lograr los objetivos planteados. Sabemos que hay una distinción muy fina, pero ayudaría tener más claro qué persigue la agenda frente a la política propuesta.

De otra parte, también creemos que al Ministerio de Defensa se le están asignando tareas que, en general, podrían cuestionarse. Si consideramos que este ministerio tiene como objetivos principales "la formulación y adopción de las políticas, planes generales, programas y proyectos del Sector Administrativo Defensa Nacional, para la defensa de la soberanía, la independencia y la integridad territorial", entonces, podría enmarcarse su mandato de seguridad digital a acciones operativas para la defensa del ciberespacio nacional, a la defensa de infraestructuras, actividades y funciones críticas, a la cooperación cibernética con otras entidades gubernamentales e internacionales en materia de ciberdefensa, además de a la necesidad de elevar sus capacidades cibernéticas con fines de defensa y seguridad nacional, y ejecutar ciberejercicio de protección del ciberespacio nacional. Sin duda, todas estos objetivos juegan un papel primoridal en la política.

No vemos como adecuado que el Ministerio de Defensa tenga a su cargo la actividad 2 de la Línea de Acción 7 del Objetivo específico 4.3.3. Es decir, nos resulta sospecho que quede en manos de esta entidad el ajuste a un marco legal de seguridad digital cuando se integran tecnologías emergentes (ej. big data, inteligencia artificial, etc.). Parece una actividad más propia de entidades no militares. Lo mismo se puede decir de la actividad a su cargo de crear una estrategia que ayude a mejorar la seguridad digital de la cadena de suministros de bienes y servicios TI (actividad 4 de la Línea de Acción 10).

Finalmente, nos sigue llamando la atención que no se incluya ninguna actividad que permita hacer una evaluación independiente sobre los pro y contra de mantener el colCERT suscrito al Ministerio de Defensa. En caso de que la evaluación concluya la conveniencia de tener un colCERT independiente, debería además incluir una hoja de ruta para que esto suceda. Esta actividad podría estar a cargo del Coordinador Nacional. Hasta tanto esto no ocurra, nos seguirá preocupando la injerencia del Ministerio de Defensa en aspecto relacionados con la creación e implementación de un modelo de divulgación coordinada de vulnerabilidades.

Otros aspectos

Adecuación del marco legal al Convenio de Budapest

RECOMENDACIÓN

Distinguir entre funciones de prevención, relacionadas con la seguridad digital, y de persecución de delitos, relacionadas con el sector justicia, para tratar la adecuación

del marco legal al Convenio de Budapest de forma independiente a la política de seguridad digital.

Sabemos que cuando se habla de ciberdelito, en general, se piensa en aquellas conductas delictivas que solo pueden ocurrir en línea: el robo de datos de identidad, por ejemplo, o el uso de *ransomware*. Sin embargo, hoy es difícil imaginar un delito moderno que no implique, en algún momento de su ejecución, el uso de un computador, de un sistema informático o red. Por este motivo, creemos que la Línea de Acción 6 debería dirigirse a permitir que la adaptación del marco legal al Convenio de Budapest se incorpore en la política criminal en materia de prevención del crimen. A fin de cuentas, este tratado prevé que el ciberdelito pueda significar "todo delito". Un enfoque de este tipo podría ayudar a establecer una mejor estrategia de prevención de ciberdelitos.

Adecuación del marco legal de derechos humanos

RECOMENDACIÓN

Reemplazar la Línea de Acción 7 por la realización de un diagnóstico exahustivo de la situación de derechos humanos en relación con la seguridad digital en un proceso de participación insitucional y ciudadano amplio, a cargo del Ministerio de Justicia y Derecho.

Nos preocupa la redacción de la actividad 1 de la Línea de Acción 7 del Objetivo específico 4.3.3, dado su ambigüedad sobre el tipo de cambio que se busca y el alto riesgo para el ejercicio de derechos humanos en internet. No se ha demostrado en el diagnóstico que acompaña al Conpes que haya necesidad de revisar el marco normativo de derechos fundamentales. Antes de ordenar la adecuación del marco legal, es necesario un diagnóstico exhaustivo a cargo de los ministerios de Justicia y Derecho y de las Tecnologías de la Información y las Comunicaciones, con la colaboración de otras entidades relevantes y un proceso amplio de participación ciudadana.

Mecanismos de participación de múltiples partes interesadas

RECOMENDACIÓN

Incluir mecanismos de participación ciudadana amplios y adecuados para la presentación de insumos y discusión de propuestas en relación con las accions de la política.

Reconocemos que este borrador hace un esfuerzo loable por corregir las falencias identificadas en la implementación del CONPES de 2016 en el sentido de crear mecanismos de participación

de multiples partes interesadas. En este sentido, queremos llamar la atención a la necesidad de que también se priorice espacios de participación ciudadana adecuados y amplios cuando se presenten diagnósticos y propuestas de adecuación de marcos legales. Cualquier proceso de diagnóstico, formulación y aprobación de marcos legales debe estar guiados, además, por un enfoque de derechos humanos. Algunas de las líneas de acción que ofrecen la oportunidad de involucrar a la ciudadanía en las dicusiones de seguridad digital son la línea de acción 2 sobre Agenda Nacional de Seguridad Digital y la mencionada Línea de Acción 7 sobre adecuación del marco legal a derechos humanos.

Enfoques diferencia y de género

RECOMENDACIÓN

Transversalizar los enfoques diferencial y de género contenido en la Línea de Acción 12 para toda la política de seguridad digital, la Agenda Nacional de Seguridad Digital y la adecuación de marcos normativos a derechos humanos.

Como señalamos previamente, nos complace que el borrador haya identificado como falla la no incorporación de enfoques diferencias y de género en materia de seguridad digital. No obstante, queremos resaltar que la actividad 2 dentro de la Línea de Acción 12, a cargo del Ministerio de las Tecnologías de la Información y las Comunicaciones, de diseñar una estrategia con estos enfoques para elevar la participación en el ámbito de seguridad digital debe aplicar a todos los programas de competencia y capacidades que se proponen en el documento. Si esos enfoques se consiguen extender a las demás actividades del Conpes, se estaría apostando por una visión mucho más inclusivo en materia de seguridad digital.

Rutas coordinadas de divulgación de vulnerabilidades

RECOMENDACIÓN

Revisar la adecuación institucional, estratégica y del marco legal para hacer posible la creación de ruta de divulgación confiables y apropiadas.

Celebramos que este documento haya escuchado nuestra preocupación[4] sobre la falta de rutas coordinadas de divulgación de vulnerabilidad en el país y que se esté planteando actividades para corregir los problemas identificados. Como hemos evidenciado, la estrategia de seguridad digital debe optar por el camino de la divulgación coordinada de vulnerabilidades y reducir el riesgo jurídico de las personas que quieren contribuir a la seguridad de las infraestructuras y sistemas nacionales.

[4] Fundación Karisma. (2019). *Estudio sobre rutas de divulgación de vulnerabilidades de seguridad digital*. Disponible en https://stats.karisma.org.co/descargar/estudio-sobre-rutas-de-divulgacion-en-seguridad-digital-2/.

Tomar en serio la necesidad de la divulgación coordinada de vulnerabilidades exige cambios institucionales y normativos, así como es necesaria para fortalecer las capacidades instituciones, organizaciones y ciudadanía en relación con la seguridad digital. La incorporación de esta forma de colaboración entre las múltiples partes interesas requiere una revisión de las líneas de acción en todos los puntos estratégicos de la política. Queremos destacar especialmente algunos puntos que tocan los tres primeros objetivos específicos de la política.

En primer lugar, como hemos mencionado, es necesario definir con claridad las competencias de las distintas instituciones que hacen parte de la gobernanza de la seguridad digital. La definición de competencias debe distinguir entre el papel de instituciones como MinTIC, Delegatura de Protección de Datos Personales y los distintos centros de resupuesta a incidentes dentro de la ruta de divulgación para generar confianza en quienes encuentrar vulnerabilidades y quieren colaborar con su mitigación y eliminación. Si bien el colCERT está inscrito al Ministerio de Defensa, debería reducirse al máximo su involucramiento, de manera que cualquier protocolo, modelo y mecanismo de reporte genera la mayor confianza posible entre el público interesado.

En segundo lugar, la Agenda Nacional de Seguridad Digital y las funciones de la autoridad máxima en este tema debe incluir competencias y facultades para establecer la coordinación de las distintas entidades para producir una ruta de divulgación segura.

Finalmente, la adecuación del marco legal debe tener en cuenta los riesgos jurídicos a los que actualmente se expone quien encuentra una vulnerabilidad y quiere divulgarla de forma responsable. La evaluación de las necesidades de reforma normativa debe tener en cuenta esta actividad y conectar a través del diagnóstico y la evaluación de las distintos modelos de divulgación a entidades como Ministerio de Defensa y la Fiscalía General de la Nación, así como la Rama Judicial.

Mecanismos de rendición de cuentas

RECOMENDACIÓN

Crear mecanismos participativos de rendición de cuentas de las actividades esbozadas en la política.

Nos preocupa que el documento no crea mecanismos de rendición de cuentas por las actividades designadas a las diferentes entidades. Quizá es una actividad que pueda delegarsele al Coordinador Nacional, la creacion de mecanismos participativos de rendición de cuenta.

Observatorio para medir y monitorear niveles de confianza y seguridad digital

RECOMENDACIÓN

Eliminar la actividad del obervatorio de la Línea de Acción 10, mantendiéndola dentro de la Línea de Acción 13.

Esta actividad está repetida en las Líneas de Acción 10 y 13. Nos parece más adecuado que quede dentro de la Línea de Acción 13.